

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平8-149449

(43)公開日 平成8年(1996)6月7日

(51)Int.Cl.⁶ 識別記号 庁内整理番号 F I 技術表示箇所
H 0 4 N 7/167
5/00 B
5/91

H 0 4 N 7/ 167 Z
5/ 91 P

審査請求 未請求 請求項の数 2 O L (全 9 頁) 最終頁に続く

(21)出願番号 特願平6-284730

(22)出願日 平成6年(1994)11月18日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 早川 弘之

神奈川県横浜市戸塚区吉田町292番地株式
会社日立製作所マルチメディアシステム事
業部

(72)発明者 橘 浩昭

神奈川県横浜市戸塚区吉田町292番地株式
会社日立製作所マルチメディアシステム事
業部

(74)代理人 弁理士 小川 勝男

最終頁に続く

(54)【発明の名称】 デジタル信号蓄積伝送装置

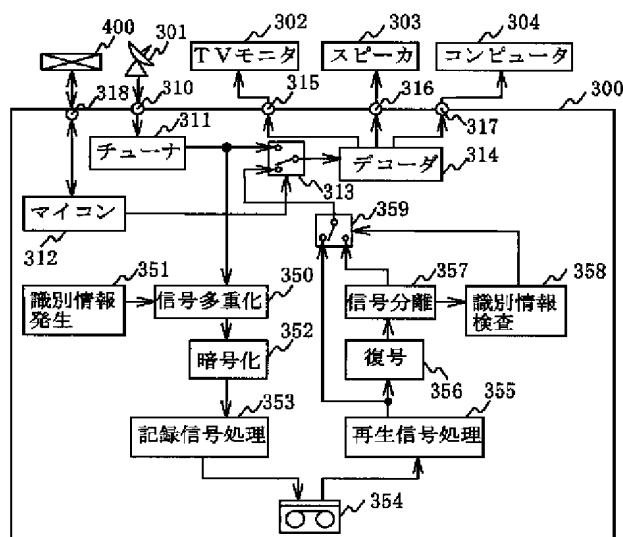
(57)【要約】

【目的】本発明の目的は、蓄積伝送する情報に対して固有の識別情報を付加し、暗号化して蓄積伝送することにより、再生或いは受信した情報の視聴を特定の装置に制限することで、情報の著作権やプライバシー情報を保護することが可能となるデジタル信号蓄積伝送装置を提供することにある。

【構成】蓄積伝送する情報に対し固有の識別情報を付加350し、暗号化352し、蓄積伝送354し、復号356し、識別情報を分離357判定358し、識別情報が一致した場合のみ復号した情報を出力する。

【効果】情報の著作権やプライバシー情報を保護することが可能となるデジタル信号蓄積伝送装置を提供することができる。

図 2



【特許請求の範囲】

【請求項1】 デジタル信号を入力するデジタル信号入力手段と、
固有の識別情報を発生する識別情報発生手段と、
該識別情報発生手段より出力された識別情報と上記デジタル信号入力手段に入力されたデジタル信号とを多重化する信号多重化手段と、
該信号多重化手段の出力信号を暗号化する暗号化手段と、
該暗号化手段の出力する暗号化信号を蓄積伝送する蓄積伝送手段と、
上記蓄積伝送手段より再生又は伝送された暗号化信号を復号する復号手段と、
該復号手段により復号した信号中から識別情報とデジタル信号を分離する信号分離手段と、
該信号分離手段により分離された識別情報が固有の識別情報と一致するか否かを検査する識別情報検査手段と、
該識別情報検査手段の出力する制御信号に応じて、上記信号分離手段の出力するデジタル信号と上記蓄積伝送手段より再生又は伝送された暗号化信号のいずれかを選択して出力する信号選択手段と、
該信号選択手段の出力信号を出力するデジタル信号出力手段とを有し、
上記信号分離手段により分離された識別情報が固有の識別情報と一致した場合、上記信号選択手段は上記信号分離手段の出力するデジタル信号を選択して出力し、
上記信号分離手段により分離された識別情報が固有の識別情報と一致しない場合、上記信号選択手段は上記蓄積伝送手段より再生又は伝送された暗号化信号を選択して出力することを特徴とするデジタル信号蓄積伝送装置。

【請求項2】 デジタル信号を入力するデジタル信号入力手段と、
固有の識別情報を発生する識別情報発生手段と、
該識別情報発生手段より出力された識別情報と上記デジタル信号入力手段に入力されたデジタル信号とを多重化する信号多重化手段と、
該信号多重化手段の出力信号を暗号化する暗号化手段と、
該暗号化手段の出力する暗号化信号を蓄積伝送する蓄積伝送手段と、
上記蓄積伝送手段より再生又は伝送された暗号化信号を復号する復号手段と、
該復号手段により復号した信号中から識別情報とデジタル信号を分離する信号分離手段と、
該信号分離手段により分離された識別情報が固有の識別情報と一致するか否かを検査する識別情報検査手段と、
該識別情報検査手段の出力する制御信号に応じて、上記信号分離手段から入力されたデジタル信号を出力するか否かを決定するスイッチ手段と、
該スイッチ手段の出力信号を出力するデジタル信号出力

手段とを有し、
上記信号分離手段により分離された識別情報が固有の識別情報と一致した場合のみ、上記スイッチ手段は上記信号分離手段の出力するデジタル信号を出力することとを特徴とするデジタル信号蓄積伝送装置。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】 本発明は、デジタル信号を蓄積伝送するデジタル信号蓄積伝送装置に関し、特に蓄積伝送されるデジタル信号の著作権やプライバシー情報を保護しつつ、デジタル信号の蓄積や伝送を可能とするのに適したデジタル信号蓄積伝送装置に関する。

【0002】

【従来の技術】 映像信号に対しスクランブル処理を施して記録媒体に記録を行う記録再生装置に関する技術は、例えば、特開平4-86177に記載されている。

【0003】

【発明が解決しようとする課題】 上記の従来技術には、アナログ映像信号の映像部分に対しスクランブル処理を施した上で、識別情報を同期信号部分に付加し、記録媒体に記録を行う記録再生装置に関する技術について述べられている。

【0004】 しかしながら、デジタル化し圧縮符号化した映像信号や音声信号、その他のデータ等のデジタル信号を多重化したビットストリームを、蓄積媒体に蓄積したり通信網を用いて伝送する際、これらのデジタル信号の著作権やプライバシー情報を保護しつつ、デジタル信号の蓄積や伝送を可能とする方法及び技術については何ら開示されていない。

【0005】 本発明の目的は、デジタル信号の著作権やプライバシー情報を保護しつつ、デジタル信号の蓄積や伝送を可能とするデジタル信号蓄積伝送装置を供給することにある。

【0006】

【課題を解決するための手段】 上記目的を達成する為に、以下に示す手段を設けた。

【0007】 デジタル信号を入力するデジタル信号入力手段と、固有の識別情報を発生する識別情報発生手段と、識別情報発生手段より出力された識別情報とデジタル信号入力手段に入力されたデジタル信号とを多重化する信号多重化手段と、信号多重化手段の出力信号を暗号化する暗号化手段と、暗号化手段の出力する暗号化信号を蓄積伝送する蓄積伝送手段と、蓄積伝送手段より再生又は伝送された暗号化信号を復号する復号手段と、復号手段により復号した信号中から識別情報とデジタル信号を分離する信号分離手段と、信号分離手段により分離された識別情報が固有の識別情報と一致するか否かを検査する識別情報検査手段と、識別情報検査手段の出力する制御信号に応じて、信号分離手段の出力するデジタル信号と蓄積伝送手段より再生又は伝送された暗号化信号の

いずれかを選択して出力する信号選択手段、又は識別情報検査手段の出力する制御信号に応じて、信号分離手段の出力するデジタル信号を出力するか否かを決定するスイッチ手段と、信号選択手段又はスイッチ手段の出力信号を出力するデジタル信号出力手段とを設ける。

【0008】

【作用】デジタル信号をデジタル信号入力手段により入力する。

【0009】また、識別情報発生手段により、固有の識別情報を発生する。

【0010】信号多重化手段でこの識別情報とデジタル信号入力手段に入力されたデジタル信号とを多重化し、暗号化手段でこれを暗号化し、蓄積伝送手段に蓄積伝送する。

【0011】次に、蓄積伝送手段より再生又は伝送された暗号化信号を復号手段で復号し、信号分離手段で識別情報とデジタル信号を分離する。

【0012】識別情報検査手段において、信号分離手段により分離された識別情報が固有の識別情報と一致するか否かを検査し、検査結果に応じて信号選択手段に対して制御信号を出力する。

【0013】信号選択手段は、この制御信号に応じて、信号分離手段の出力するデジタル信号と蓄積伝送手段より再生又は伝送された暗号化信号のいずれかを選択して出力する。

【0014】信号分離手段により分離された識別情報が固有の識別情報と一致した場合、信号選択手段は信号分離手段の出力するデジタル信号を選択して出力する。そして、信号分離手段により分離された識別情報が固有の識別情報と一致しない場合、信号選択手段は蓄積伝送手段より再生又は伝送された暗号化信号を選択して出力する制御を行う。

【0015】また、信号選択手段の代わりにスイッチ手段を設けた場合には、識別情報検査手段が出力する制御信号に応じて、信号分離手段から入力されたデジタル信号を出力するか否かを決定する。つまり、信号分離手段により分離された識別情報が固有の識別情報と一致した場合のみ、スイッチ手段は信号分離手段の出力するデジタル信号を出力する制御を行う。

【0016】その結果、信号分離手段により分離された識別情報が、記録時の固有の識別情報と一致した時のみ、復号したデジタル信号は出力されるので、蓄積伝送されたデジタル情報は、固有の識別情報を有する特定の装置でしか再生することができない。再生可能な装置を制限することで、蓄積伝送されたデジタル信号の契約外の視聴や違法複製による視聴を防止し、蓄積及び／又は伝送されたデジタル信号の著作権を保護することができる。

【0017】また、蓄積伝送されるデジタル信号中に多重化されている識別情報も、暗号化されているため、蓄

積伝送されるデジタル信号からは識別情報を知ることができず、より信頼性の高いセキュリティを提供することができる。さらに、暗号化及び復号のアルゴリズムは、全ての装置共通とすることができるので、安価な装置を供給することができる。

【0018】本発明によれば、入力されたデジタル信号に対し、固有の識別信号を多重し暗号化し蓄積伝送する構成とすることで、蓄積伝送したデジタル信号の再生可能な装置を制限することができ、デジタル信号の著作権やプライバシー情報を保護しつつ、デジタル信号の蓄積や伝送を可能とするデジタル信号蓄積伝送装置を供給することができる。

【0019】

【実施例】本発明の一実施例を図1に従い説明する。図1に示す実施例では、本発明を適用した多チャンネル有料デジタル放送の受信端末を含む通信衛星を利用した多チャンネル有料デジタル放送システムについて説明する。図1は、通信衛星を利用した多チャンネル有料デジタル放送のシステム構成を示すブロック図である。図1において、100は放送センタ、200は放送衛星、300は受信端末、400は電話回線である。

【0020】通信衛星を利用した多チャンネル有料デジタル放送では、情報を圧縮して伝送することで、同一回線で大きなチャンネル数を確保することができる。

【0021】デジタル化された映像信号や音声信号などを圧縮伝送する標準として、例えば、MPEGやH.261等が提案及び規格化されているが、本実施例では、MPEG2 (Moving Picture Experts Group phase 2、メディア統合系動画画像圧縮の国際標準)を例に上げて説明する。

【0022】通信衛星を利用した多チャンネル有料デジタル放送ではその大きなチャンネル数を利用して、同じ番組を複数のチャンネルで一定時間毎、時間をずらして放送するタイムシフト放送や、受信端末のリクエストに応じて番組を放送するビデオオンデマンド、電話回線と組み合わせたテレビショッピング、テレビゲームのアプリケーションプログラムやデータの配信、などの新サービスが可能となる。また信号自身をデジタルで伝送受信できるため劣化がなく高品質の情報を得ることができる。

【0023】放送局100から送出された情報、例えば、圧縮された映像信号や音声信号、文字情報、アプリケーションソフトウェア、データなどは、通信衛星200を介して、各受信端末300へ送られる。

【0024】また、ビデオオンデマンドやテレビショッピングなどのアプリケーションでは、受信端末300と接続された電話回線400を介して、放送局100に対しリクエストや申込みを行う。そして、放送局100は、電話回線400を介して各受信端末300の課金情報を集計し、視聴料を請求することができる。

【0025】図2は、図1に示した受信端末300の内部構成を示すブロック図である。

【0026】図2において、300は図1に示した受信端末、301は受信アンテナ、302はTVモニタ、303はスピーカ、304はコンピュータ、310は受信信号入力端子、311はチューナ、312はマイコン、313はスイッチ、314はデコーダ、315は映像信号出力端子、316は音声信号出力端子、317はデータ出力端子、318は電話回線接続端子、350は信号多重化回路、351は識別情報発生回路、352は暗号化回路、353は記録信号処理回路、354は磁気テープ及びVTR機構、355は再生信号処理回路、356は復号回路、357は信号分離回路、358は識別情報検査回路、359はスイッチ、400は電話回線である。

【0027】通信衛星を利用した多チャンネル有料デジタル放送では、信号をデジタルで伝送受信できるため劣化がなく高品質の情報を得ることができる。しかしながら、劣化がなく、複製の容易なデジタル情報を得られることにより、複製が大量に行われるようになると、海賊版が横行し、著作権が侵害されたり、プライバシー情報の漏洩など、正常な有料放送の運営が破綻を来すだけでなく、社会問題を引き起こす可能性がある。したがって、著作権やプライバシー情報を保護し、正常な運営を行うために放送局は、送出する番組にスクランブルを掛けて送出し視聴可能な端末を制限するのが一般的になっている。

【0028】受信アンテナ301を用い通信衛星からの信号を受信する。受信アンテナ301で受信した信号は、受信信号入力端子310を介してチューナ311へ入力される。受信端末300内のチューナ311では、復調の他、降雨落雷など通信障害によるデータの欠落や誤りを訂正補完し出力する。図2では省略してあるが、受信したデータが、複数のチャンネルを時分割多重化している場合、マイコン312の発行するコマンドに従い、マイコン312の指定したチャンネルと受信したMPEGデータのトランスポートパケット内に含まれるパケットIDを比較し、両者が一致したトランスポートパケットのみを選択して出力する。

【0029】現在、通信衛星からの信号を受信中である場合には、マイコン312はスイッチ313の出力にチューナ311からの入力を選択するようコマンドを発行する。スイッチ313ではマイコン312からのコマンドに従い、入力を切り替え、チューナ311からの入力信号を出力する。

【0030】スイッチ313から出力されたデータは、デコーダ314へ入力される。図2では省略してあるが、デコーダ314はデスクランブラと、MPEG等の伸張処理回路、信号形式変換回路から構成されており、デコーダ314に入力されたデータにスクランブルが掛

けられている場合、この入力されたデータはデスクランブラで解読される。このデスクランブラは、放送センタ100から送られてくるデータのスクランブルを解読するためのデスクランブラであり、視聴の制限が目的であり契約外的不正視聴を防止するためのものである。

【0031】そして、デスクランブルされたデータはMPEGなど各種データに対応した伸張処理回路で伸張され、信号形式変換回路で出力する再生装置の特性に応じた形式に変換され、例えば、映像信号は映像信号出力端子315を介してTVモニタ302へ、音声信号は音声信号出力端子316を介してスピーカ303へ、アプリケーションソフトウェア、データはデータ出力端子317を介してコンピュータ304へ出力される。

【0032】ビデオオンデマンドなどのアプリケーションでは、複数の受信端末300からのリクエストに対し、限られたチャンネル数で同時に対応する必要がある。例えば、1つのプログラムを実演時間かかって送信すると、1つの受信端末300が実演時間分1つのチャンネルを占有することになり、非常に効率が悪い。そこで、帯域圧縮を施した1つのプログラムに対し、さらに時間軸圧縮を行い、実演時間より短い時間で送出することで、チャンネルの占有時間を減らし、数多くの受信端末300のリクエストに対応することができるようになる。しかし、時間軸圧縮を行ってデータを送信した場合、大量のデータが短い時間で送られて来るため受信端末300側に受信したデータを一時的に保存する記憶媒体が必要となる。また、受信したデータを一時的に記録媒体に記録した場合、早送り巻戻し、一時停止、可変速再生などが受信端末300側で行うことができるようになり、視聴者の見たい時間にマイペースでみることができるようになる等のメリットも生じる。

【0033】短時間に送られてくる大量のデータを一時的に記録する記録媒体として、デジタルVTR、DAT (Digital Audio Tape recorder)、光磁気ディスク、ハードディスク、メモリアレイなどを使うことが可能であるが、本実施例ではデジタルVTRを例にあげて説明する。

【0034】チューナ311からのデータは、信号多重化回路350に入力される。信号多重化回路350では、チューナ311から入力されたデータ中から、トランスポートパケットの先頭と示す8ビットの同期バイトを検出して、チューナ311から入力されたデータを、188バイトのトランスポートパケット単位に分割し、この188バイトのトランスポートパケット毎それぞれに、識別情報発生回路351から入力された例えば4バイトの識別情報を付加し202バイトのブロックデータとして出力する。

【0035】信号多重化回路350から出力された202バイトのブロックデータは、暗号化回路352に入力される。暗号化回路352では、例えば、擬似乱数発生

回路があり、この擬似乱数発生回路で発生させた擬似乱数と暗号化回路352に入力されたデータとの排他的論理和をとることで、入力されたブロックデータを暗号化し出力する。

【0036】暗号化されたブロックデータは、記録信号処理回路353に入力される。記録信号処理回路353では、入力されたブロックデータに対し、同期データやブロックアドレス、パリティ符号を付加してパケット化し、さらに、パケット化したデータを、例えば、磁気テープ等の記憶媒体に記録再生できるようデジタル変調して出力し、磁気テープ354に記録する。

【0037】一方、磁気テープ354から再生された信号は、再生信号処理回路355に入力される。再生信号処理回路355では、再生された信号を復調し、同期データを検出しパケット化されたデータ中から、暗号化された202バイトのブロックデータを抽出する。また、同時に記録したパリティ符号を用いて、データの誤りを訂正し出力する。

【0038】再生信号処理回路355から出力された202バイトのブロックデータは復号回路356に入力される。復号回路356では、暗号化回路352と同じ擬似乱数発生回路があり、擬似乱数発生回路で発生させた擬似乱数と入力された暗号化データとの排他的論理和をとり、暗号化された202バイトのブロックデータを復号し出力する。

【0039】復号したデータは信号分離回路357に入力される。信号分離回路357では、復号されたデータ中から信号多重化回路350で多重化された4バイトの識別情報と188バイトのトランスポートパケットとを分離して出力する。信号分離回路357で分離された4バイトの識別情報は識別情報検査回路358に入力される。識別情報検査回路358では、磁気テープ354から再生され信号分離回路357で分離出力された識別情報と識別情報発生回路351から出力される識別情報を比較し、比較結果に応じたコマンドを発行しスイッチ359に対し出力する。

【0040】スイッチ359は、識別情報検査回路358から出力されるコマンドに従って入力を切り替えて出力する。つまり、信号分離回路357で分離出力された識別情報と識別情報発生回路351から出力される固有の識別情報が一致したことを示すコマンドが入力された場合、スイッチ359は信号の入力に信号分離回路357で分離出力されたトランスポートパケットを選択し出力する。一方、信号分離回路357で分離出力された識別情報と識別情報発生回路351から出力される固有の識別情報が一致しないことを示すコマンドが入力された場合、再生されたデータは違法に複製されたデータまたは契約外の端末300で再生されたデータであると判定し、このコマンドが入力されたスイッチ359は、入力に再生信号処理回路355から出力される復号されてい

ないデータを選択して出力する。この場合MPEGのフォーマットを守っていないデータが出力されるため伸張処理ができず再生された情報は視聴することはできない。

【0041】現在、磁気テープ354に記録されたデータを再生中である場合には、マイコン312はスイッチ313の出力にスイッチ359からの入力を選択するようコマンドを発行する。スイッチ313ではマイコン312からのコマンドに従い、入力を切り替え、スイッチ359からの入力信号を出力する。

【0042】スイッチ313から出力されたデータはデコード314に入力される。デコード314では、入力されたデータがスクランブルデータである場合、デスクランブラで解読され出力される。また、デコード314内のMPEGデコードでトランスポートパケットから、画像データ、音声データ、その他のデータを分離し、伸張処理し出力する。そして、デコード314内の信号形式処理回路で、例えば映像データであれば、パソコンモニタに出力する場合RGBデータに変換し、テレビに出力する場合NTSCやPAL、ハイビジョン等の信号形式に変換して、映像信号出力端子315を介しTVモニタ302へ出力する。また、音声データであれば、D/Aコンバータによりアナログ信号に変換し音声信号出力端子316を介しスピーカ303へ出力する。そして、コンピュータやゲームのアプリケーションデータの場合、RS-232CやSCSIで伝送できるようボーレートを合わせたりやパリティや制御信号を付加してデータ出力端子を介してコンピュータ304へ出力する。

【0043】通信衛星200からの信号を受信した場合や磁気テープ354に情報を記録した場合、磁気テープ354から情報を再生した場合などそれぞれに合わせた課金情報が、例えば、マイコン312内のフラッシュROMに記憶される。この課金情報は、放送センタ100が電話回線400及び電話回線接続端子318を介し、例えば定期的にアクセスすることで課金情報を集計し、契約している加入者に対し課金する。

【0044】また、マイコン312及び電話回線接続端子318、電話回線400を介し、例えば、ビデオオンデマンドやテレビショッピングなどのリクエストを送信することができる。

【0045】以上に説明したように、記録するデジタル情報に対し、識別情報を付加しさらに暗号化して、記憶媒体に記録することで、識別情報自身も暗号化されているため、識別情報を知ることができず、システムの安全性を確保することができる。さらに、例えば、上記に示した回路を集積して1チップのLSIにして、再生された識別情報が各受信端末300固有の識別情報と一致しない場合に、復号されたデータがLSIの外部に取り出せない構成とすることで、さらなるシステムの安全性を確保することができ、部品点数を削減することで、安価

な受信端末300を提供することができる。

【0046】また、受信端末300内の暗号化回路352及び復号回路356は、通信衛星を利用した多チャンネル有料デジタル放送を受信し記録した情報の再生を、特定の契約者のみに制限するための機能である。上記に示した回路構成とすることで、受信し蓄積した情報が違法に複製され、また契約外の状況で再生され、情報の著作権やプライバシー情報が侵害されるのを防止することができる。

【0047】次に、本発明の二実施例を図3に従い説明する。図3に示す二実施例では、図1に示した一実施例と同様に、本発明を適用した多チャンネル有料デジタル放送の中継局及び受信端末を含む通信衛星を利用した多チャンネル有料デジタル放送システムについて説明する。

【0048】図3において、100は放送センタ、200は放送衛星、380は受信端末、400は電話回線、500は中継局、550はケーブルネットワークである。

【0049】山間地や離島などの難視聴地域にのみならず、近年の都市部における建築構造物の密集化や建築構造物の高層化や地下化に伴い、一実施例に示したようなシステムでは、通信衛星200からの電波を直接受信できないなどの都市部における難視聴地域の発生が社会問題化している。

【0050】そこで、図3に示した二実施例のように、通信衛星200からの電波を中継局500で共同受信し、中継局500と各受信端末380の間に張り巡らされたケーブルネットワーク550を介して通信衛星200からの電波を受信及び配信するシステムも構築されている。ケーブルネットワーク550は、例えば、光ケーブルや同軸ケーブルで専用回線を敷設したり、広帯域ISDN(Integrated Service Digital Network)の電話回線を利用したり、都市型のCATV(Cable Television)ネットワークを利用する等などの方法がある。

【0051】公共回線など他のシステムと混在して使用される場合には、一実施例で示したシステムと同様に伝送される情報のセキュリティ、つまり著作権やプライバシー情報の保護が重要な課題となる。

【0052】次に図4を用いて、図3に示した中継局500と受信端末380の内部構成とその動作について説明する。

【0053】図4において、図2の構成要素と均等なものには同一符号を付し、その説明は重複を避けるため割愛する。380は図3に示した受信端末、381は受信信号入力端子、382は受信信号処理回路、500は中継局、501は送信信号処理回路、502は送信信号出力端子、550はケーブルネットワークである。

【0054】通信衛星200からの電波を中継局500

に設置したアンテナ301で共同受信する。アンテナ301からの信号は、受信信号入力端子310を介し、中継局500内のチューナ311に入力される。中継局500内のチューナ311では、復調の他、降雨落雷など通信障害によるデータの欠落や誤りを訂正補完し、MP EG2の形式である188バイトのトランスポートパケット単位のデータとして出力される。チューナ311から出力されたデータは、信号多重化回路350に入力される。

【0055】一方、識別情報発生回路351では視聴可能な視聴者の識別番号を連続して発行し、188バイトから成る識別情報パケットを構成する。識別情報パケットの先頭の4バイトは、ヘッダー情報が書き込まれており、同期バイト、識別情報パケットを示すビット、識別情報パケットの総数とその識別情報パケットのアドレスを示す情報などから構成されている。このヘッダー情報に続いて、視聴可能な視聴者の識別番号を例えば差分を取り可変長符号化してビット圧縮された識別番号情報、訂正符号が続く形で識別情報パケットが構成される。

【0056】信号多重化回路350では、チューナ311から入力される受信したトランスポートパケットと、識別情報発生回路351から入力される識別情報パケットを、パケット単位で多重化して出力する。

【0057】信号多重化回路350から出力された多重化データは、暗号化回路352に入力される。暗号化回路352では、例えば、擬似乱数発生回路があり、この擬似乱数発生回路で発生させた擬似乱数と暗号化回路352に入力された多重化データとの排他的論理和をとることで、入力された多重化データを暗号化し出力する。

【0058】暗号化された多重化データは送信信号処理回路に入力され、188バイトのパケット単位で、同期バイト、パケットアドレス、パリティビット等が付加され、例えば、光ケーブルへ送信するための信号に変調され、光信号に変換され、送信信号出力端子502を介して、ケーブルネットワーク550に出力される。

【0059】次に、ケーブルネットワーク550からの信号を、ケーブルネットワーク550に接続された複数の受信端末380で受信する。

【0060】以下で説明する受信端末380は、図1及び図2に示した受信端末300のように大量のデータを蓄積する記憶媒体を備えていない。受信端末300から蓄積装置の機構を削減し簡易な構成とすることで、より安価な受信端末を提供することができる。また、二実施例に示す受信端末380でも、受信端末300のように蓄積装置を備えることは可能であるが、一実施例の説明と重複を避けるため蓄積装置を装備しない形を用いて説明する。

【0061】ケーブルネットワーク550からの信号は、光ケーブルからの光信号を電気信号に変換し復調する。そして、同期バイトを検出し、パケットの先頭を検

出し、パケットの先頭位置をもとにパケットアドレス、パリティビットを検出し、これらを検査し、通信障害によるデータの欠落や誤りを訂正補完し出力する。

【0062】そして、受信信号処理回路382から出力された暗号化データは復号回路356に輸入される。復号回路356では、暗号化回路352と同じ擬似乱数発生回路があり、擬似乱数発生回路で発生させた擬似乱数と入力された暗号化データとの排他的論理和をとり、暗号化された188バイト単位のトランスポートパケットを復号し出力する。

【0063】復号したトランスポートパケットは信号分離回路357に輸入される。信号分離回路357では、受信したトランスポートパケットが複数のチャンネルを時分割多重化している場合、マイコン312の発行するコマンドに従い、マイコン312の指定したチャンネルと受信したMPEGデータのトランスポートパケット内に含まれるパケットIDを比較し、両者が一致したトランスポートパケットのみを選択してスイッチ359に対して出力する。

【0064】また、識別情報パケットを示すビットが検出された場合、そのパケットは識別情報パケットであると認識して、識別情報パケットのみを分離して、識別情報検査回路358に対して出力する。

【0065】識別情報検査回路358では、188バイトから成るを構成されている識別情報パケット中に含まれている訂正符号により、データ誤りを検出し訂正する。さらに、先頭の4バイトのヘッダー情報に含まれている識別情報パケットの総数とその識別情報パケットのアドレスを示す情報をもとに、複数の識別情報パケットに渡るデータをつなぎ合わせ可変長符号化されたデータを復号する。

【0066】そして、復号された識別情報の中に、各受信端末380固有の識別情報が含まれているか検査する。各受信端末380固有の識別情報は、例えば、識別情報検査回路358に付加されているROM(Read Only Memory、読みだし専用メモリ)に記憶されている。ROMから出力された各受信端末380固有の識別情報と、復号された識別情報を比較し、復号された識別情報中に各受信端末380固有の識別情報が含まれていた場合、出力許可を示すコマンドを発行して出力する。

【0067】一方、復号された識別情報を比較し、復号された識別情報中に各受信端末380固有の識別情報が含まれていない場合、出力拒否を示すコマンドを発行して出力する。

【0068】スイッチ359は、識別情報検査回路358から入力されるコマンドに従って回路の接続/切断を実行する。つまり、識別情報検査回路358から出力許可を示すコマンドが輸入された場合、スイッチ359は、信号分離回路357から入力されるMPEGのトランスポートパケットを出力する。一方、識別情報検査回

路358から出力拒否を示すコマンドが輸入された場合、マイコン312に対し出力拒否を示すコマンドが輸入されたことを知らせ、スイッチ359は回路を切断して、信号分離回路357から入力されるMPEGのトランスポートパケットは出力しない。

【0069】スイッチ359の出力信号は、デコーダ314に輸入される。図4では省略してあるが、デコーダ314はデスクランブラと、MPEG等の伸張処理回路、信号形式変換回路から構成されており、デコーダ314に輸入されたデータにスクランブル掛けられている場合、この入力されたデータはデスクランブラで解読される。このデスクランブラは、放送センタ100から送られてくるデータのスクランブルを解読するためのデスクランブラであり、契約外の視聴を制限するためのものである。

【0070】そして、出力拒否を示すコマンドが発行され、スイッチ359から信号が出力されない場合、マイコン312はデコーダ314を介し、例えば、TVモニタに警告を表示させる等の処理を行う。結果として、デコーダ314にデータが輸入されないため、契約外や違法の受信端末380ではデータを復号することができず、不正視聴を防止し、情報の著作権を保護することができる。

【0071】一方、出力された識別情報と識別情報発生回路351から出力される識別情報が一致している場合、スイッチ359の輸入は信号分離回路357からの入力が出力されているため、復号回路356で復号されたトランスポートパケットが出力されている。

【0072】したがって、デコーダ314では、入力されたデータがスクランブルデータである場合、デコーダ314内のデスクランブラで解読され出力される。また、MPEGデコーダでトランスポートパケットから、映像データ、音声データ、その他のデータを分離し、伸張処理し出力する。

【0073】そして、デコーダ314内の信号形式処理回路で、例えば映像データであれば、パソコンモニタに出力する場合RGBデータに変換し、テレビに出力する場合NTSCやPAL、ハイビジョン等の信号形式に変換して、映像信号出力端子315を介しTVモニタ302へ出力する。

【0074】また、音声データであれば、D/Aコンバータによりアナログ信号に変換し音声信号出力端子316を介しスピーカ303へ出力する。そして、コンピュータやゲームのアプリケーションデータの場合、RS-232CやSCSIで伝送できるようボーレートを合わせたりやパリティを付加してデータ出力端子を介してコンピュータ304へ出力する。

【0075】通信衛星200からの信号を受信した場合、利用に合わせた課金情報が、例えば、マイコン312内のフラッシュROMに記憶される。この課金情報

は、放送センタ 100 が電話回線 400 及び電話回線接続端子 318 を介し、例えば定期的に受信端末 380 をアクセスすることで課金情報を集計し、契約している加入者に対し課金する。

【0076】また、マイコン 312 及び電話回線接続端子 318、電話回線 400 を介し、例えば、ビデオオンデマンドやテレビショッピングなどのリクエストを送信することができる。

【0077】上記、一実施例及び二実施例において放送センタ 100 から送信されてくるデータは、スクランブルが掛けられている場合について説明した。しかしながら、スクランブルが掛けられない無料放送もあり、これらを受信して記録したりまたは再送信した場合でも、記録時や送信時に暗号化し、再生可能な装置を制限することで放送される情報の著作権を保護することが可能となる。

【0078】

【発明の効果】本発明によれば、蓄積伝送する情報に対して固有の識別情報を付加し、暗号化して蓄積及び又は伝送し、再生或いは受信した情報を復号し、識別情報を分離し、特定の識別情報が含まれていた場合のみ、復号した情報を出力することにより、再生或いは受信した情報の視聴を特定の装置に制限することで、蓄積伝送する情報の著作権やプライバシー情報を保護することが可能となるデジタル信号蓄積伝送装置を提供することができる。

【図面の簡単な説明】

【図 1】本発明の一実施例を適用した多チャンネル有料デジタル放送の受信端末を含む通信衛星を利用した多チャンネル有料デジタル放送システム全体を示す構成図で

ある。

【図 2】図 1 に示した多チャンネル有料デジタル放送の受信端末 300 の内部構成を示すブロック図である。

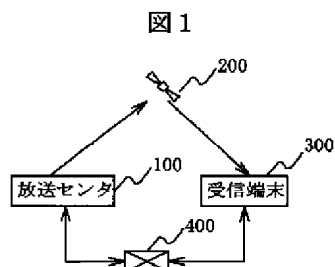
【図 3】本発明の二実施例を適用した多チャンネル有料デジタル放送の中継局及び受信端末を含む通信衛星を利用した多チャンネル有料デジタル放送システム全体を示す構成図である。

【図 4】図 3 に示した多チャンネル有料デジタル放送の中継局 500 及び受信端末 380 の内部構成を示すブロック図である。

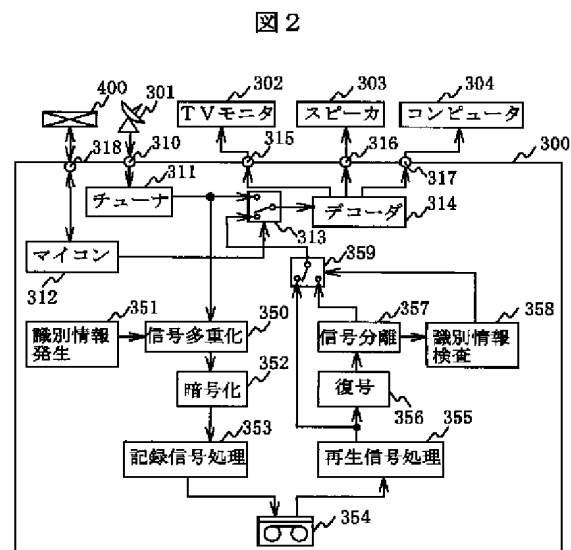
【符号の説明】

100…放送センタ
200…放送衛星
300…受信端末
302…TV モニタ
303…スピーカ
304…コンピュータ
311…チューナ
314…デコーダ
350…信号多重化回路
351…識別情報発生回路
352…暗号化回路
356…復号回路
357…信号分離回路
358…識別情報検査回路
380…受信端末
400…電話回線
500…中継局
550…ケーブルネットワーク

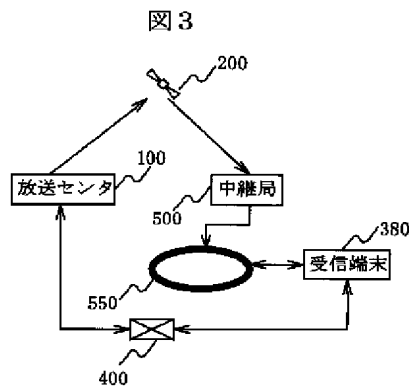
【図 1】



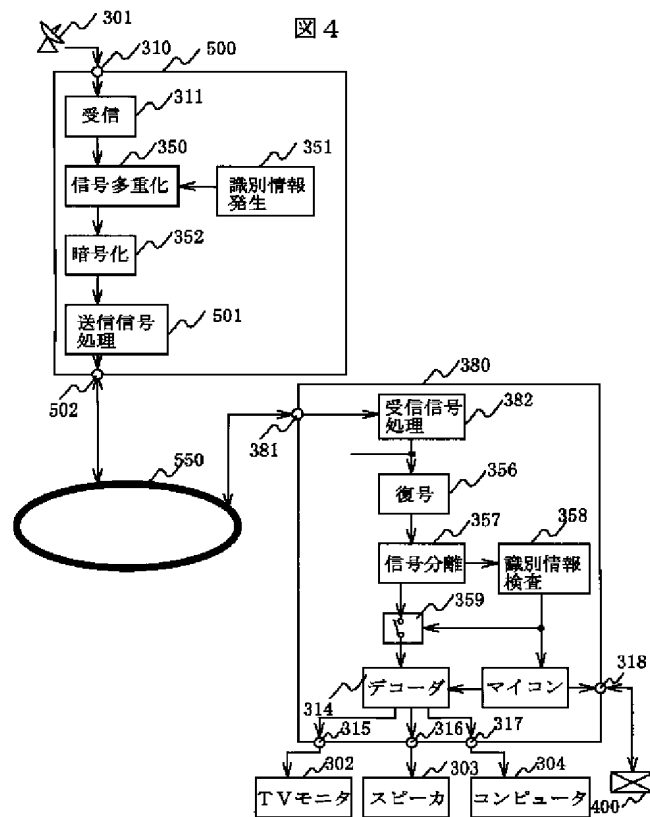
【図 2】



【図3】



【図4】



フロントページの続き

(51)Int.Cl.⁶

H 0 4 N 5/92

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 N 5/92

H

(72)発明者 細川 恭一

神奈川県横浜市戸塚区吉田町292番地株式
会社日立製作所映像メディア研究所内

(72)発明者 吉澤 和彦

神奈川県横浜市戸塚区吉田町292番地株式
会社日立製作所映像メディア研究所内